(19) Europäisches Patentamt
European Patent Office
Office uropéen d s br vets

(11) Numéro de publication : **0 626 793 A1**

(12) DEMANDE DE BREVET EUROPEEN

(21) Numéro de dépôt : **94112343.2**

(22) Date de dépôt : **14.04.87**

(51) Int. Cl.[5] : **H04N 7/167**

Cette demande a été déposée le 08 - 08 - 1994 comme demande divisionnaire de la demande mentionnée sous le code INID 60.

(30) Priorité : **18.04.86 CH 1576/86**

(43) Date de publication de la demande : **30.11.94 Bulletin 94/48**

(60) Numéro de publication de la demande initiale en application de l'article 76 CBE : **0 243 312**

(84) Etats contractants désignés : **BE CH DE ES FR GB IT LI NL SE**

(71) Demandeur : **NAGRA PLUS S.A.**
22, route de Genève
CH-1033 Cheseaux-sur-Lausanne (CH)

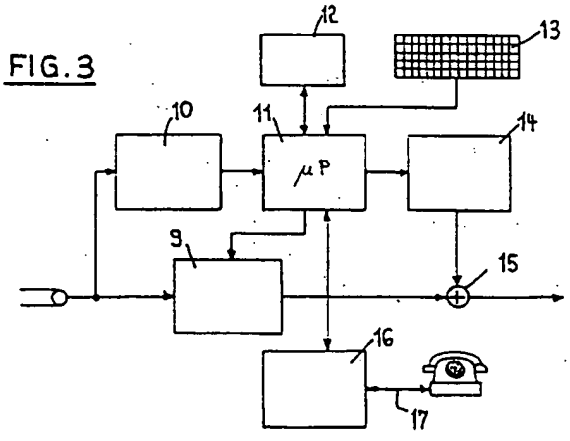
(72) Inventeur : **Kudelski, André**
Chemin de la Crésentine 21
CH-1023 Crissier (CH)
Inventeur : **Laffely, Laurent**
chemin du Mottier 4
CH-1052 Le Mont-sur-Lausanne (CH)
Inventeur : **Sasselli, Marco**
chemin des Roches 6
CH-1803 Chardonne (CH)

(74) Mandataire : **Cronin, Brian Harold John**
c/o GRIFFES CONSULTING SA
70, route de Florissant
CH-1206 Genève (CH)

(54) Système de télévision à péage.

(57) Un système de télévision à péage comprend, au niveau de la réception, un décodeur et une carte séparée (12) pouvant être connectée au décodeur, le décodeur recevant à la fois un signal vidéo brouillé et un code de débrouillage chiffré. Le décodeur inclut une mémoire (9) destinée à stocker un signal vidéo qui parvient au décodeur de façon débrouillée, et un premier microprocesseur (11) destiné à commander ladite mémoire (9) pour débrouiller le signal vidéo, ce premier microprocesseur (11) étant en liaison avec la carte séparée (12). Cette carte (12) inclut un second microprocesseur (40) avec mémoire (41, 42, 43) destiné à stocker des codes relatifs à des émissions achetées, à recevoir le code de débrouillage et transmettre au décodeur l cod de débrouillage déchiffré. Ce décod ur utilise alors l code de débrouillage déchiffré pour débrouill r, à l'aide de la mémoire (9), le signal vidéo brouillé et p rmettre ainsi un affichag en clair d l'émission diffusée.

FIG.3



EP 0 626 793 A1

La présente invention concern un système de télévision à péage, comprenant, au niv au d la récepti n, un décodeur et une cart séparée pouvant être connectée audit décod ur, le décod ur recevant à la fois un signal vidéo brouillé et un code de débrouillage chiffré.

Dans un système de télévision à péage (pay-TV), et de manière générale, l'abonné choisit les programmes qu'il désire regarder et il paie pour recevoir ces programmes qui sont transmis sous forme brouillée afin d'être inintelligibles aux non abonnés ou aux abonnés qui n'ont pas choisi ni payé pour un programme particulier. Les signaux peuvent être transmis par câble, antenne ou satellite. Les systèmes de télévision à péage évolués comportent en outre la possibilité dite "pay-per-view" d'achat de programmes soit juste avant le début de l'émission, soit en cours d'émission, et ceci dans un système de transmission à voie unique. Dans ce cas, il est nécessaire de mémoriser un certain crédit à l'endroit de l'utilisateur, crédit qui est à disposition pour permettre l'achat et la réception d'une émission pay-per-view que l'on désire regarder. Si le crédit mémorisé est suffisant, le montant de l'émission est débité du crédit et le signal reçu de la station émettrice est débrouillé pour en p rmettre une réception confortable.

Le document W0 81/02499 concerne un procédé et un système pour le brouillage de la transmission d'information vidéo, particulièrement pour la télévision à péage. Des parties du signal vidéo, par exempl des parties ou segments de lignes, des lignes ou d s trames sont transmises dans un ordre différent de leur séquence naturelle. La manière de réarranger la séquence des segments de lignes pour la transmission peut être contrôlée par un générateur de code qui change la séquence à chaque trame ou en fonction d'une autre base de temps adéquate. Le code, qui peut être chiffré, varie de manière aléatoire et il peut être entièrement ou partiellement transmis avec le signal vidéo brouillé.

Le brevet US 4 484 217 concerne un procédé et un système pour facturation à distance d'un programm de télévision à péage. Le crédit à disposition est mémorisé à l'endroit du souscripteur et un signal de coût est transmis par l'émetteur. Pay-per-view est rendu possible par le fait qu'il est prévu un achat impulsif. Un code unique peut accompagner le signal émis dans un but d'identification. Si le décodeur du souscripteur reconnaît le programme comme un programme d'achat par impulsions, le coût du programme est affiché. Pour visualiser le programme, le souscripteur ntre un demande adéquat dans le décodeur et celui-ci compar automatiquem nt le coût du programme avec le crédit disponibl . Si le coût n'excède pas l crédit, l programm est débrouillé t le coût est déduit du crédit. Cependant, le système ci-dessus n'est pas prévu pour permettre l'affichage sous forme d télétexte d'informations émis s relatives aux émissions prévues, dans leur ordre chronologiqu , ni l'affichage d'informations sous forme d'instructions pour les opérations à eff ctuer par l'utilisateur sur le décodeur afin de faciliter l dialogu entre celui-ci et l'utilisateur et éviter d s erreurs de manipulation.

En conséquence, le but de la présente invention est d'améliorer la gestion de crédit dans un système de télévision à péage. Dans ce but, le décodeur du système inclut :

- une mémoire destinée à stocker un signal vidéo qui parvient au décodeur de façon brouillée et à libérer ledit signal vidéo d'une façon débrouillée; et
- un premier microprocesseur destiné à commander ladite mémoire pour débrouiller ledit signal vidéo, ce premier microprocesseur étant en liaison avec ladite carte.

En outre, ladite carte inclut :

- un second microprocesseur avec mémoire destiné à stocker des codes relatifs à des émissions achetées, à recevoir ledit code de débrouillage et transmettre au décodeur ledit code de débrouillage déchiffré; ce décodeur utilisant alors ledit code de débrouillage déchiffré pour débrouiller, à l'aide de ladite mémoire, ledit signal vidéo brouillé et permettre ainsi un affichage en clair de l'émission diffusée.

L'invention va être expliquée ci-après à l'aide de la description d'une forme d'exécution illustrée dans le dessin.

La figure 1 montre le principe fondamental d'un système de télévision à péage,

La figure 2 montre le principe de l'entrée et de la sortie d'une ligne du signal vidéo parmi les 32 lignes, par exemple, d'un buffer,

La figure 3 montre un schéma bloc du décodeur selon l'invention,

La figure 4 montre le principe du chiffrement et déchiffrement des codes de débrouillage transmis,

La figure 5 montre la rotation d'une ligne du signal vidéo,

La figure 6 montre l'inversion d'une ligne du signal vidéo,

La figure 7 montre une symétrie miroir d'une ligne du signal vidéo,

La figure 8 montre un schema-bloc de la carte CPTV,

La figure 9 montre la structure physique d'une ligne du signal vidéo,

La figure 10 montre la structure des donné s physiques dans le systèm de transmission de données Didon, et

La figure 11 montre la structure des d nnées dans l système Didon.

En figure 1, un micro-ordinat ur 1 est prévu p ur générer des données selon un format de télétexte relatives aux programmes des émissions prévues telles

que titre, prix, date ou période d'émission, etc. ainsi que d'autres informations utiles à l'utilisateur. Ces données sont introduites en 3 par un interface 2 dans le signal vidéo délivré par une caméra 4 ou tout autre élément producteur de signal vidéo. Les lignes du retour du balayage vertical du signal vidéo qui ne transmettent normalement aucune information sont utilisées pour transmettre les données de télétexte, de sorte que celles-ci sont transmises en même temps que le signal vidéo.

La figure 9 montre la structure d'une ligne de retour du balayage vertical du signal vidéo. On voit que la ligne est formée de 32 bytes de données de télétexte et qu'elle comprend en outre des informations de synchronisation et des adresses en code Hamming pour la détection/correction d'erreurs. Les 32 bytes de données de télétexte sont protégées par 2 bytes de code de détection d'erreurs CRC-16.

Dans cet exemple, le signal vidéo avec les données de télétexte est ensuite délivré à un brouilleur 5 qui permet de brouiller l'image, par exemple par permutation des lignes ou par d'autres moyens. Le signal brouillé est transmis par voie hertzienne, par câble vidéo ou par satellite au récepteur 6 du souscripteur. Le récepteur comporte un débrouilleur 7 qui délivre le signal débrouillé au téléviseur 8.

Le signal brouillé est entièrement compatible avec les normes SECAM et PAL(NTSC). Le brouillage peut être exécuté en version normale ou en version profonde. En version normale, les lignes vidéo sont permutées entre elles, seule la partie active de la ligne étant permutée. Dans le système PAL(NTSC), le burst (fréquence porteuse couleur) est laissé inchangé. Chaque ligne est échantillonnée et digitalisée sur 8 bits à une fréquence d'échantillonnage $f = 3 \times f_{burst}$ ou $f = 4 \times f_{burst}$ à la fréquence ligne, de sorte que dans le système PAL(NTSC), la phase couleur est conservée. Chaque ligne est ainsi divisée en principe en 3 (ou 4)x 256 segments de 8 bits. La figure 4 montre le principe du brouillage et débrouillage des signaux vidéo transmis. A l'émission, un générateur de hasard 25 produit des mots de code en temps réel. Une information 26 relative à l'identification de l'émission à transmettre est délivrée avec une clé de transmission 34 et le mot de code à un système de chiffrage 27, qui délivre en temps réel le signal chiffré 28 à transmettre. La clé de transmission 34 peut être transmise sous forme codée. A la réception, le signal transmis est délivré avec la clé de transmission au système de déchiffrage 29, par exemple selon le système DES qui délivre le mot de code déchiffré (pour autant que l'émission en cours ait été acheté) à l'information d'identification 26. Le mot de code commande un générateur de pseudo hasard 30 qui délivre à son tour des points adresses 31 pour une table 32 de 256 codes de permutation. A chaque ligne du signal vidéo, la table sélectionne parmi 32 buffers celui qui permet la dé-permutation des lignes.

Il est possible d'entrer et sortir les lignes du buffer dans un ordre quelconque. La figure 2 montre schématiquement une mémoire buffer 18 comprenant les 3 x 256 segments 19 de 8 bits formant une ligne du signal vidéo. Dans cette mémoire, les segments ou échantillons sont introduits séquentiellement dans des positions successives de la mémoire. La figure montre que l'introduction d'un nouveau segment 20 dans une des positions de la mémoire libère le segment 21 qui était stocké dans cette position, de sorte que la mémoire est toujours remplie de 32 lignes et qu'un buffer est toujours rempli de 256 segments. Le brouillage/débrouillage tel qu'indiqué ci-dessus, offre une excellente sécurité contre le piratage pour les raisons suivantes :

- Le nombre de permutations de lignes possibles est si grand qu'il est difficile de trouver la "bonne combinaison", soit par hasard, soit par corrélation.
- Le code ou clé de permutation est transmis en temps réel, de sorte que même si un pirate trouve la bonne permutation, celle-ci n'est valable que pour un instant, par exemple une seconde.
- Le code de permutation est transmis chiffré, par exemple mais non exclusivement, selon le système DES, pratiquement incassable.
- Le déchiffrage des codes de permutation se fait dans une carte intelligente à microprocesseur (carte CPTV), comme on le verra plus loin, offrant toute la sécurité nécessaire. Selon l'invention, le microprocesseur de la carte constitue un des éléments du décodeur.
- Les cartes CPTV sont reprogrammables, ce qui permet de changer périodiquement les clés de codage.

Dans la version brouillage profond, on effectue en plus de la permutation des lignes comme indiqué ci-dessus, un ou plusieurs des brouillages suivants :

- selon figure 5, une rotation de la ligne active sur elle-même, c'est-à-dire par exemple que la partie active de la ligne commence au milieu de la vraie ligne et est suivie, après la fin de la vraie ligne, du début de cette même ligne,
- selon figure 6, une inversion de la polarité de la ligne active par rapport au niveau correspondant à 50 IRE. Cette opération permet d'effectuer une adaptation automatique du niveau de luminosité pour garder celui-ci constant. Ceci permet de supprimer la possibilité de reconnaissance d'image par changement de l'éclairage ambiant.
- selon figure 7, une symétrie miroir de la ligne vidéo selon laquelle la partie active de la ligne vidéo subit une symétrie axiale d'axe perpendiculaire au niveau noir de la vidéo.

Rappelons encore que lors du brouillage, seule la partie active de la ligne est permutée, y compris ou

non les lign s de retour du balayag vertical, ce qui permet le brouillage d s données de télétexte, mais que dans tous les cas, la synchronisation horizontale reste inchangée. A la sortie du buffer, les donné s sont r conv rties en signaux analogiques par un convertisseur numérique/analogique de 8 bits. On obtient ainsi un signal SECAM ou PAL(NTSC) débrouillé pour affichage sur le téléviseur. Examinons maintenant le principe du décodeur et ses possibilités d'utilisation.

La figure 3 montre que le signal vidéo en provenance de la station de tête (émettrice) est délivré à la mémoire buffer vidéo 9 de 32 lignes permettant d'effectuer la dé-permutation des lignes comme indiqué ci-dessus et à un récepteur de données de télétexte 10. Rappelons ici que les données en format de télétexte sont transmises en même temps et par le même canal que le signal vidéo, ces données étant transmises par les lignes de retour du balayage vertical du signal vidéo. Un microprocesseur 11 est l'élément central du décodeur. Il comprend des mémoires mortes et vives pour toutes les informations susceptibles d'êtr affichées sur le téléviseur, ces informations qui s nt en forme de données en format de télétexte, étant en partie transmises par la station de tête et mémorisées dans une mémoire vive du microprocesseur et en partie mémorisées dans une mémoire morte du microprocesseur 11. Le microprocesseur est associé à une carte de sécurité dite CPTV (carte Pay TV) 12 normalement insérée dans le décodeur et à un clavier 13 de celui-ci. Le microprocesseur délivre, sur appel à l'aide du clavier, les données de télétexte sous forme numérique adéquate à un générateur de texte 14 commandant l'affichage du téléviseur. Le microprocesseur 11, en liaison avec la carte CPTV 12, c mmande le buffer 9 pour dépermuter les lignes comme indiqué précédemment. Le signal vidéo débrouillé ainsi que celui du générateur de texte sont à disposition en 15 pour être affichés sur le téléviseur. En utre, le microprocesseur peut aussi être relié à un m dem 16 connecté lui-même à une ligne téléphonique 17.

Examinons maintenant plus en détail les possibilités du décodeur décrit ci-dessus.

La carte CPTV est une carte active comprenant un microprocesseur muni de manière interne d'une mémoire non volatile (RAM avec pile, NVRAM ou E-2PROM) illisible de l'extérieur (sécurité) et une horlog . Selon figure 8, la carte comprend deux circuits électroniques A et B : le circuit A est un dispositif de sécurité av c CPU 40 et mémoires associé s telles qu ROM 41, E2PROM 42, RAM 43, ainsi qu'un interface de mémoire 44, et l circuit B est une mémoire séparé E2PROM de 2 Kbytes. La cart se présente en principe sous la form d'un carte de crédit. Ell rassemble les quatre fonctions suivantes :

- Décodage de la clé d permutation transmis cryptée, par exemple selon le système DES. La cart reçoit du microprocesseur 11 la clé cryptée et r tourne, lorsque l'émission a été acheté , la clé de débrouillage permettant de dépermuter les lignes du signal vidéo.
- Mémorisation de la liste des numéros, ou codes des émissions achetées et des abonnements à un genre particulier d'émissions (émissions sportives, culturelles, cinéma, cuisine, etc.). Cette mémorisation de la liste des émissions achetées permet à la carte CPTV de ne retourner au microprocesseur le code de débrouillage que si l'émission a bien été achetée. En outre, et dans un but de statistique et de facturation, il est possible de connaître les émissions achetées.
- Gestion du crédit. La carte CPTV mémorise une information représentative du crédit qu'elle peut utiliser pour l'achat d'émissions ou d'abonnements. Pour acheter une émission, l'utilisateur fait apparaître, par action sur le clavier 13, la liste des émissions prévues reçues au préalable de la station de tête et mémorisées dans le microprocesseur 11 du décodeur et qui sont sélectionnées par menu et affichées sur l'écran du téléviseur. Le téléviseur affiche, en plus du titre de l'émission, son numéro, prix, date d'émission et d'autres informations utiles si nécessaire. L'utilisateur sélectionne alors le numéro de l'émission qu'il désire en actionnant la touche correspondante sur le clavier. Si le crédit à disposition mémorisé dans la carte est suffisant pour l'achat en question, l'émission ou l'abonnement acheté est mémorisé dans la carte sur la liste des émissions achetées et le montant correspondant est déduit du crédit disponible. Lorsque l'émission achetée est diffusée, elle est identifiée par la carte par comparaison avec son numéro ou code inscrit sur la liste des émissions achetées et la carte retourne au microprocesseur le code ou clé de débrouillage.
- La quatrième fonction de la carte CPTV est une fonction de mesure du temps par une horloge. Cette fonction est utilisée lors de certaines émissions, par exemple de jeux interactifs entre l'utilisateur et la station de tête, comme décrit plus loin.

On voit que la carte se distingue des cartes connues de l'état de la technique en ce qu'elle mémorise toutes les informations confidentielles ou secrètes nécessaires au débrouillage du signal vidéo, telles que clés de débrouillag et le crédit. La carte gère le crédit, mém ris les émissions achetées t perm t le débrouillage des émissions achetées. Elle est effaçable, toutes les donné s mémorisées pouvant être modifiées. Il est ainsi possible de modifier les clés de débrouillage et de réutiliser la carte un fois r mpli .

Pour toutes les opérations à effectuer, l'utilisa-

teur est guidé par le décodeur lui-même qui affiche des text s et instructions de manipulation sur le téléviseur par l'intermédiaire du générateur de texte 14. Dans ce but, une partie de l'information susceptible d'être affichée sous forme de texte est mémorisée en permanence dans une mémoire morte du microprocesseur 11, cette partie correspondant en principe à des instructions de manipulation, et l'autre partie des informations est mémorisée temporairement dans une mémoire vive du microprocesseur 11, cette d uxième information étant diffusée par la station de tête et concernant plus particulièrement les programmes qui seront diffusés. Les possibilités suivantes sont offertes à l'utilisateur :

- Visualisation des titres, prix, etc. des programmes qui seront diffusés,
- Guide dans l'achat des émissions programmées,
- Guide dans l'achat des abonnements (fenêtres/canaux),
- Guide dans les fonctions annexes du décodeur,
- Dialogue avec le décodeur transparent à l'utilisateur,
- Réception de messages (particuliers/généraux),
- Réception de télétexte standard.

Ce qui précède montre que le dialogue entre l'utilisateur et le décodeur est énormément facilité par dernier. Le décodeur est en outre particulièrement bien adapté à l'achat par l'utilisateur, directement chez lui, d'une émission en dialogue avec le décodeur (pay-per-view), sans en informer le centre de gestion, c'est-à-dire que toutes les opérations d'achats sont effectuées dans la carte CPTV, le décodeur interprétant les ordres donnés par l'utilisateur et les transmettant à la carte CPTV. Dans ce but, l'utilisateur sélectionne simplement à l'aide du clavier le titre de l'émission qui l'intéresse en introduisant le numéro de celle-ci et actionne une touche "validation". Si le crédit contenu dans la carte CPTV est suffisant, le numéro ou le code de l'émission choisie est mémorisé dans la liste des émissions achetées, le montant correspondant est déduit du crédit à disposition et, lorsque l'émission est diffusée, la carte délivre au microproc sseur le code de débrouillage de l'émission. Ce principe évite une suroccupation des lignes téléphoniques et permet à un utilisateur d'acheter une émission en cours.

Si le crédit contenu dans la cart est nul ou insuffisant pour l'achat d'un ab nnem nt ou d'une émission, un nouveau crédit ou un augmentation du crédit encore à disposition peut être introduit dans la carte selon l'une des possibilités suivant s:

- Achat par l'utilisateur auprès du centre de g stion d'un code (par exemple de 9 chiffres) correspondant au m ntant d crédit à recharger et recharge du crédit par introduction de ce code dans le décodeur à l'aide du clavier. Lorsque le cod est introduit dans le décodeur, le nouveau crédit est mémorisé dans la carte CPTV.
- Par échange postal de la carte à intervalles de temps régulier, ce qui permet à la station de tête de savoir quels programmes ont été regardés (statistique).
- Recharge du crédit dans un point de vente (vidéo club, banque) permettant également de savoir quels programmes ont été regardés.
- Par télécommande: le crédit de la carte peut être rechargé par antenne ou par câble sur ordre de l'émission.

Parmi les utilisations possibles du décodeur selon l'invention, mentionnons encore :

- Affichage de menus pour l'achat de programmes d'abonnement avec possibilité de connaître en tout temps les programmes achetés, ces programmes étant désignés par un signe (lettre, chiffre) particulier, affichage du crédit encore à disposition, des échéances des abonnements, de l'offre globale par la station de tête, c'est-à-dire mise à jour des programmes qui seront diffusés ultérieurement, changement des conditions par groupe d'abonnés, etc. Toutes ces informations, qui sont délivrées par le récepteur de données de télétexte (10), sont mémorisées dans les mémoires du microprocesseur 11 et affichées sur demande sur l'écran du téléviseur par le générateur de texte 14.
- Jeux interactifs: Il s'agit par exemple d'un jeu de loto avec la station de tête auquel l'utilisateur participe en misant un numéro et en introduisant le montant joué correspondant à l'aide du clavier 13. Le numéro et le montant joués sont mémorisés dans la carte CPTV. Le numéro tiré ou sorti à l'émission est transmis par le signal vidéo et sous forme codée comme données de télétexte et, si il correspond au numéro misé par l'utilisateur, celui-ci est authentifié par la carte CPTV à l'aide de l'horloge interne qu'elle contient qui détermine exactement le temps écoulé entre la mise et le contrôle du gain, pour éviter toute fraude, étant bien entendu que la mise doit précéder le tirage à l'émission. Si le joueur est gagnant, le décodeur appelle la centrale d'émission par l'intermédiaire du mod m 16 t l gain est bonifié sous forme d'un augmentation du crédit dans la carte CPTV, c tt augmentation étant commandée par la station d tête (voir ci-dessous).
- Réception d messages personnalisés émis par la station de tête. C s messages sont envoyés dans un format télétexte et l décodeur vérifie qu'il est bi n celui qui est habilité à recev ir le message. Dans ce but, chaqu carte

CPTV est porteuse d'un numéro particulier d'identification mémorisé qui est transmis station de tête avec chaque message. Si le décodeur est bien celui auquel le message est adressé, la carte permet l'affichage du message sur le téléviseur.

- Code de sécurité. Il s'agit d'un code destiné à éviter que des personnes non autorisées, par exemple des enfants, effectuent des achats dont le montant dépasse un montant prédéterminé ou participent à des jeux qui ne leur sont pas destinés. Dans ce cas, il faut introduire par le clavier un code de sécurité dans le décodeur, comme mot de passe. Si celui-ci n'est pas introduit ou si il n'est pas correct, le décodeur refuse d'exécuter l'ordre qui lui est donné.
- Liaison par modem. Grâce au modem 16 relié au microprocesseur 11 et à une ligne téléphonique 17, il est possible au décodeur dans lequel est insérée la carte CPTV, d'appeler automatiquement pendant la nuit (grâce à l'horloge de la carte CPTV) la station de tête pour se faire recharger un crédit, si celui-ci est épuisé. Par la même occasion, le décodeur envoie à la station de tête l'ensemble des émissions regardées. Bien entendu, l'appel de la station de tête par le décodeur peut aussi se faire périodiquement, à dates fixes, si désiré.
- Le décodeur peut être utilisé comme récepteur du télétexte standard avec toutes les fonctions habituelles des exploitants de chaînes de télévision ou auprès des PTT.

La figure 10 montre comme exemple de l'organisation des données dans les lignes du signal vidéo la structure des données physiques dans le cas d'une transmission de données par le système Didon (France). A chaque trame du signal vidéo est transmise une ligne telle que L0, L1, L2, L3 ou L4. Ainsi, un groupe de 5 lignes (L0 à L4) est transmis toutes les 5 trames. On voit plus particulièrement que les lignes L2 et L3 transmettent des pages de données de 32 bytes chacune. Les adressages B0 à BS permettent de sélectionner un groupe de souscripteurs parmi 2^{24} groupes, chacun de 240 souscripteurs. Les adressages comprennent le numéro du groupe, l'action à exécuter, par exemple recharge de crédit, et la liste des souscripteurs concernés par cette action particulière. La synchronisation est assurée par un reste de CRC-16 comme indiqué. En outre, chaque ligne est protégée par un CRC-16 qui permet une détection d'erreur et chaqu group d 5 lignes est protégé par un OU-EXCLUSIF qui p rmet de corriger une ligne erronée. L'avantage d'une organisati n des d nnées selon figure 10 est qu'elle p rmet de retrouver très facilement l'information là où elle se trouv dans le décodeur.

La figure 11 montre un autre exemple de structure des données dans l cas du système DI-OS (Didon operating system). On voit qu les données sont organisées en 65'536 pag s de 32 bytes chacune. Les quatre premières pag s (0 à 3) de la structure de données comprenn nt une table qui délivre pour chaque canal susceptible d'êtr transmis l'adresse de la première page d'un bloc de pages correspondant à ce canal ainsi que la longueur du bloc qui est identique avec le nombre de pages de ce bloc et le numéro des révisions ou modifications qui ont été apportées à ce bloc. L'avantage de l'organisation selon figure 11 est qu'elle conduit à une structure très souple pour la transmission des données ainsi qu'une extension future très souple.

Ce qui précède montre que le décodeur selon l'invention offre un très grand nombre de possibilités à l'utilisateur, et plus particulièrement qu'il facilite le dialogue avec ce dernier grâce à l'affichage sur le téléviseur des programmes des émissions prévues et des instructions de manipulation nécessaires à effectuer sur le clavier pour leur achat ou pour une recharge du crédit. En outre, la carte CPTV rend le décodeur extrêmement sûr contre le piratage.

Revendications

1. Système de télévision à péage, comprenant, au niveau de la réception, un décodeur et une carte séparée (12) pouvant être connectée audit décodeur, le décodeur recevant à la fois un signal vidéo brouillé et un code de débrouillage chiffré, caractérisé en ce que :

   ledit décodeur inclut :
   - une mémoire (9) destinée à stocker un signal vidéo qui parvient au décodeur de façon brouillée et à libérer ledit signal vidéo d'une façon débrouillée; et
   - un premier microprocesseur (11) destiné à commander ladite mémoire (9) pour débrouiller ledit signal vidéo, ce premier microprocesseur (11) étant en liaison avec ladite carte (12);

   et en ce que ladite carte (12) inclut :
   - un second microprocesseur (40) avec mémoire (41, 42, 43) destiné à stocker des codes relatifs à des émissions achetées, à recevoir ledit code de débrouillage et transmettre au décodeur ledit code de débrouillage déchiffré; ce décodeur utilisant alors ledit code d débrouillage déchiffré pour débrouiller, à l'aide de ladite mémoire (9), ledit signal vidéo brouillé et permettre ainsi un affichage en clair de l'émission diffusée.

2. Système de télévision à péage selon la revendication 1, caractérisé en ce que, à l'émission, des mots d code, une information (26) r lative à l'identification de l'émission à transmettr et un

clé d transmission (34) sont produits et envoyés à un système de chiffrage (27) qui délivre en temps réel le signal chiffré (28) à transmettre, et à la réc ption, le signal transmis est délivré avec la clé de transmission à un système d déchiffrage (29) qui délivre le mot de code déchiffré et l'information d'identification (26), le mot de code commandant un générateur pseudo-aléatoire (30) qui délivre à son tour des codes de débrouillage pour débrouiller dans le décodeur le signal vidéo reçu brouillé.

3. Système de télévision à péage selon la revendication 2, caractérisé en ce que ledit code de débrouillage déchiffré commande le générateur pseudo-aléatoire (30) qui délivre à son tour des pointeurs (31) pour effectuer des pointages sur une table (32) constituée par une pluralité de codes de débrouillage, de façon que les codes de débrouillage pointés soient utilisés pour commander ladite mémoire (9) afin qu'elle libère ledit signal vidéo d'une façon débrouillée.

4. Système de télévision à péage selon la revendication 1, 2 ou 3, où la mémoire (9) du décodeur est agencée pour recevoir un signal vidéo embrouillé par permutation des lignes, dans lequel chaque ligne est échantillonnée et numérisée en un nombre d'échantillons, et des moyens pour débrouiller le signal vidéo mémorisé selon un code de débrouillage variable,

caractérisé en ce que ladite mémoire (9) est constituée par un buffer de lignes (18), par exemple 32 lignes, où lesdits échantillons (20) sont introduits séquentiellement dans les cellules (19) successives, chaque ligne (18) du buffer étant constituée d'autant de cellules qui sont nécessaires pour stocker le nombre d'échantillons (20, 21) d'une ligne du signal vidéo,

l'entrée de chaque échantillon (20) dans une cellule du buffer provoquant la sortie de cette cellule de l'échantillon (21) mémorisé dans cette même cellule, de sorte que ladite mémoire (9) est toujours remplie du nombre de lignes et que chaque ligne du buffer (18) est toujours remplie du nombre d'échantillons (21 ou 20) qu'elle peut contenir,

l'ordre d'extraction des lignes du buffer mémorisées (18) pour effectuer le débrouillage étant déterminé par la sélection, sous commande dudit code de débrouillage, parmi l s lignes du buffer, d cell s qui permettent la dé-permutation des lignes.

5. Système d télévision à péag sel n la revendication 4, caractérisé en ce que chaque ligne du signal vidéo numérisé comprend 3 ou 4 fois 256 échantillons de 8 bits chacun, ces échantillons venant se stocker dans un nombre égal de cellules (19) d'une ligne (18) du buffer.

6. Système de télévision à péag selon l'une quelconque des rev ndications 4 ou 5, caractérisé en ce que le buffer comporte 32 lignes.

7. Système de télévision à péage selon l'une quelconque des revendications 4 à 6, pour le décodage d'un signal vidéo dans lequel des données sont stockées dans les lignes de retour du balayage vertical et seule la partie active de la ligne est permutée, y compris les lignes de retour du balayage vertical, la synchronisation horizontale n'étant pas permutée, de telle sorte que lesdites données sont brouillées en même temps que l'image.

8. Système de télévision à péage selon l'une quelconque des revendications 4 à 7, pour le décodage d'un signal vidéo dans lequel, en plus de la permutation des lignes, chaque ligne ainsi permutée subit en outre une rotation de la partie active de la ligne sur elle-même.

9. Système de télévision à péage selon l'une quelconque des revendications 4 à 8, caractérisé en ce que les moyens pour débrouiller le signal vidéo mémorisé comprennent : un système de déchiffrage (29) d'une carte CPTV délivrant un mot de code déchiffré, et un générateur de pseudo-hasard (30) qui délivre des pointeurs (31) à une table (32) contenant un nombre de codes de permutation, laquelle table sélectionne parmi les lignes (18) du buffer, celles qui permettent la dépermutation.

FIG.1

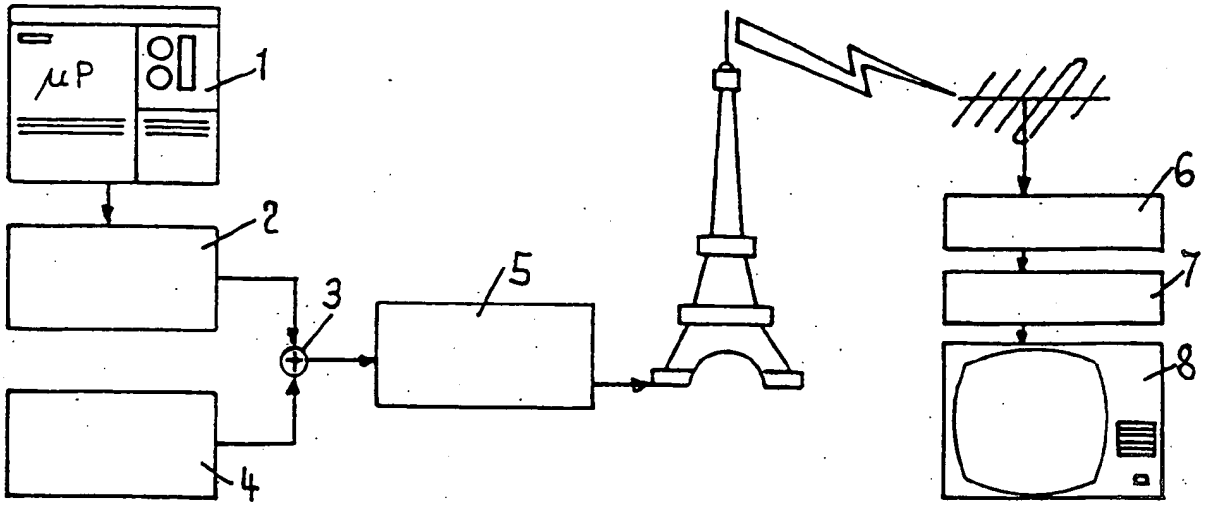


FIG.2

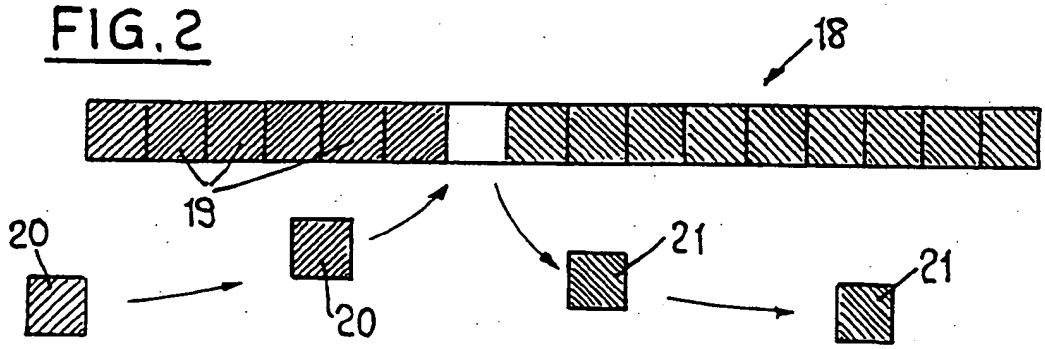
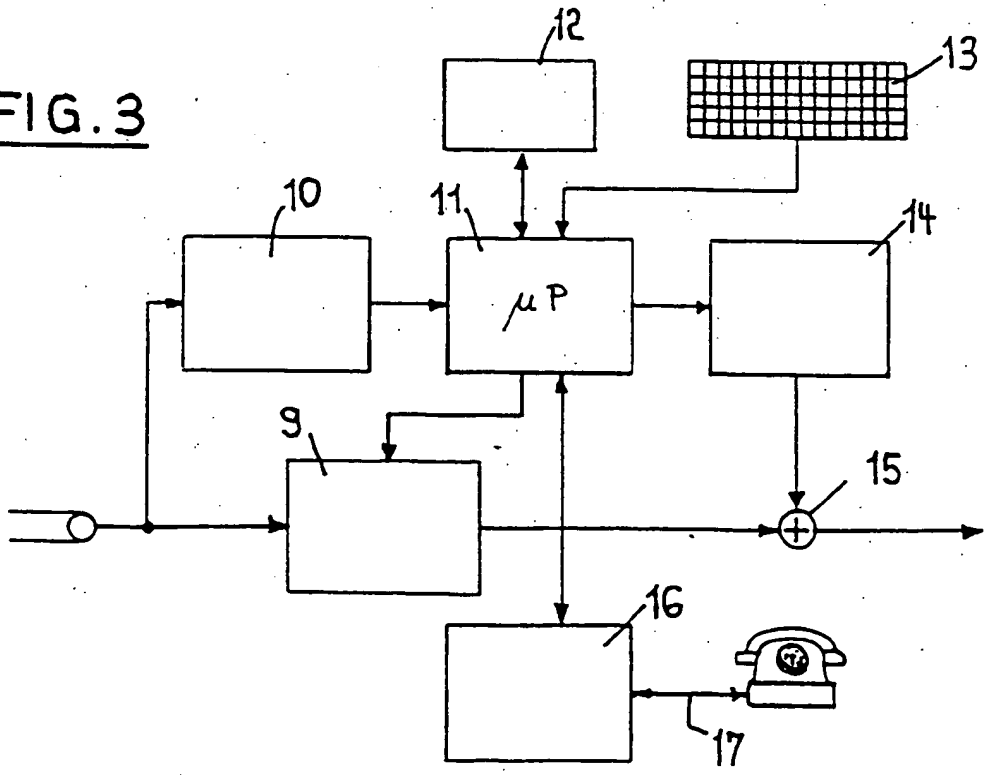


FIG.3



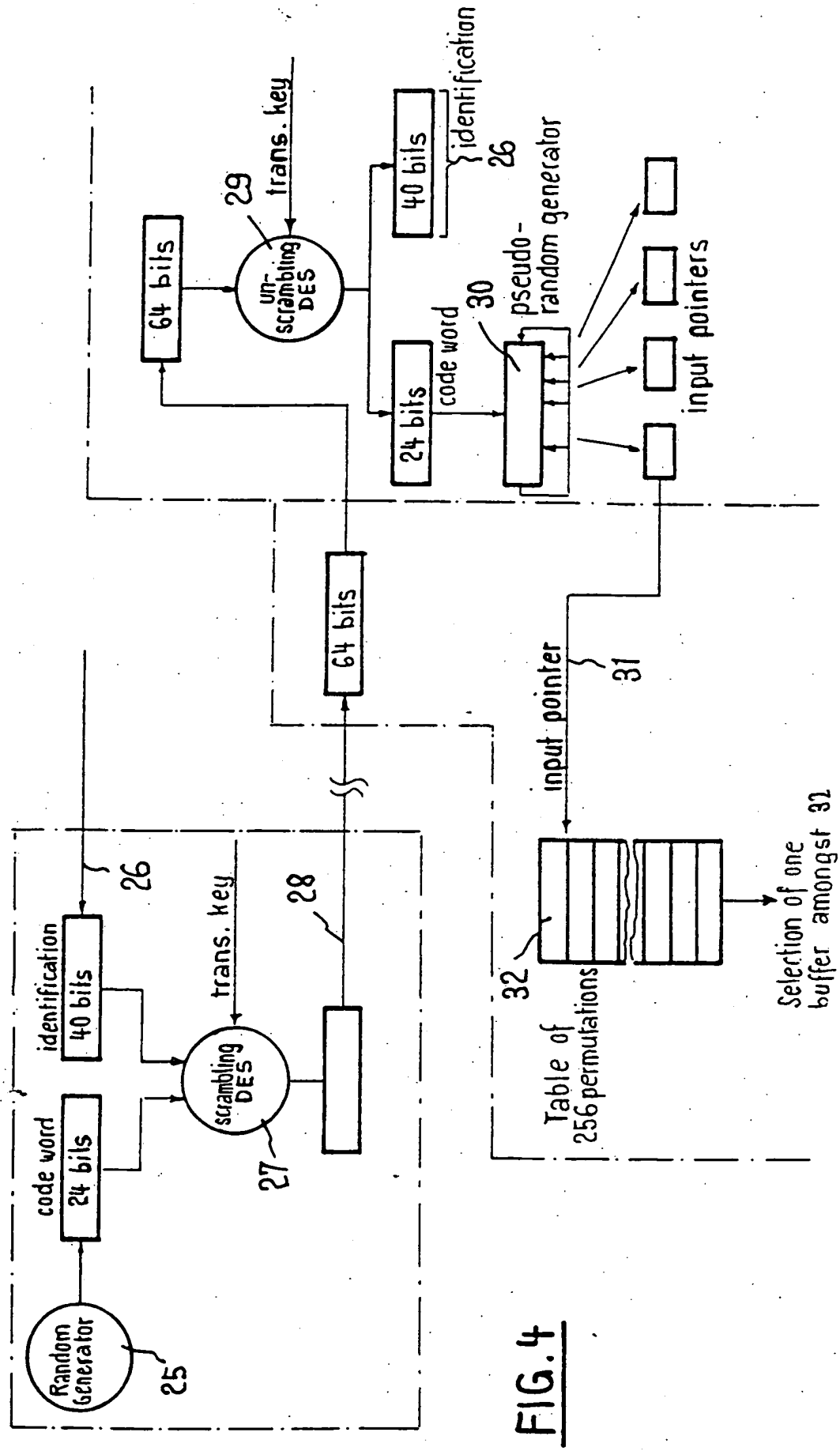

Random generator
25
code word
24 bits
identification
40 bits
26
scrambling DES
trans. key
27
28
64 bits
64 bits
un-scrambling DES
29
trans. key
40 bits
identification
26
64 bits
24 bits
code word
30
pseudo-random generator
input pointers
input pointer
31
32
Table of 256 permutations
Selection of one buffer amongst 32

FIG.4

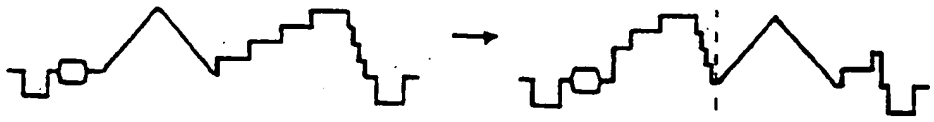


FIG.5

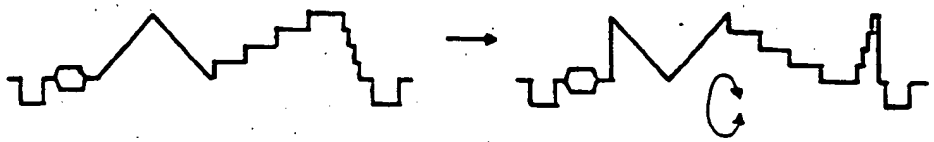


FIG.6

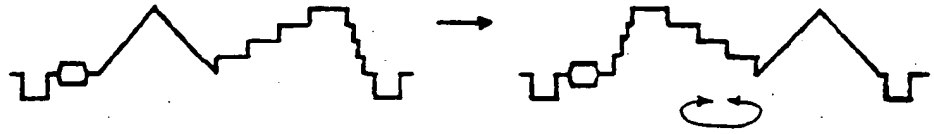
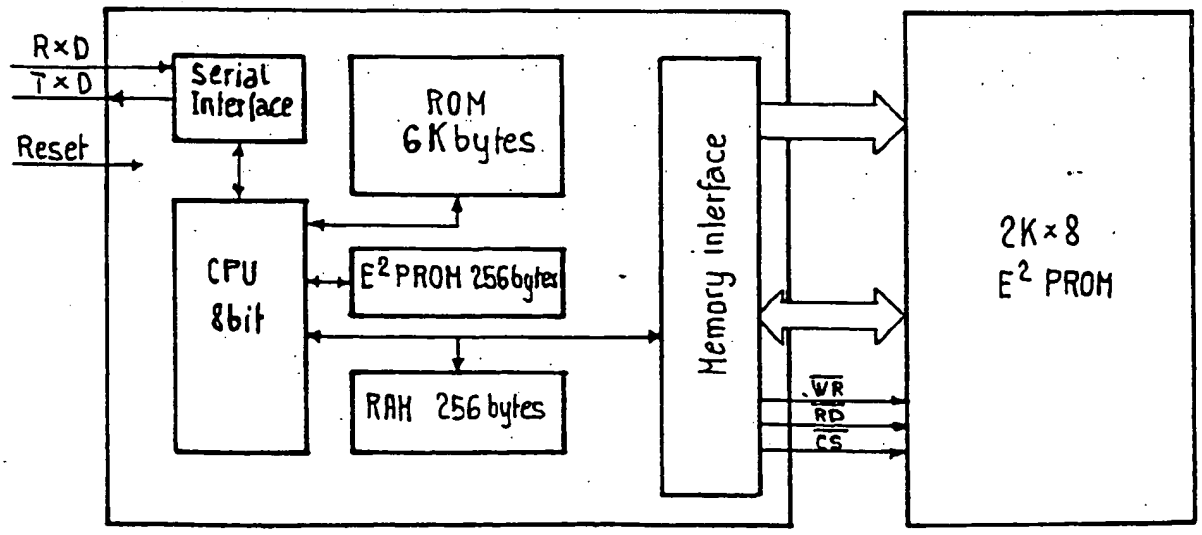


FIG.7

FIG.8



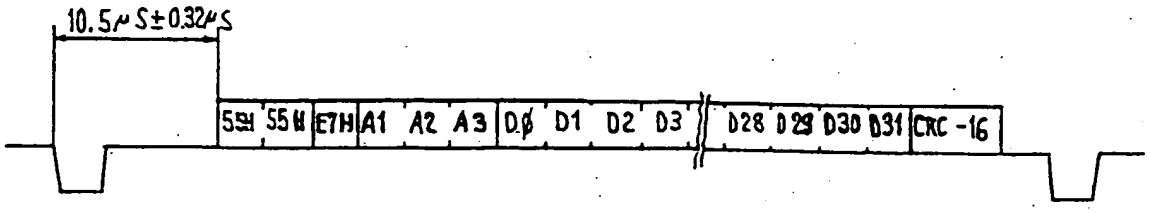


FIG.9

Caractéristiques

Vitesse de transmission:	6,203,125 Mbit/s
Code:	NRZ, AM
Mise en forme:	Sinus carré
Ligne de données:	320 bits - 40 bytes
Ordre de succession des données:	Lsb...Msb; LsB...MsB
Synchro. PLL:	2 x 55 H
Synchro. byte:	E7 H
Adresse:	A1, A2, A3 bytes en code de Hamming
Protection:	Les 32 bytes sont protégés par 2 bytes de CRC-16

Valeur Hex	Byte de Hamming							
0	0	0	0	1	0	1	0	1
1	0	0	0	0	0	0	1	0
2	0	1	0	0	1	0	0	1
3	0	1	0	1	1	1	1	0
4	0	1	1	0	0	1	0	0
5	0	1	1	1	0	0	1	1
6	0	0	1	1	1	0	0	0
7	0	0	1	0	1	1	1	1
8	1	1	0	1	0	0	0	0
9	1	1	0	0	0	1	1	1
A	1	0	0	0	1	1	0	0
B	1	0	0	1	1	0	1	1
C	1	0	1	0	0	0	0	1
D	1	0	1	1	0	1	1	0
E	1	1	1	1	1	1	0	1
F	1	1	1	0	1	0	1	0

FIG.10

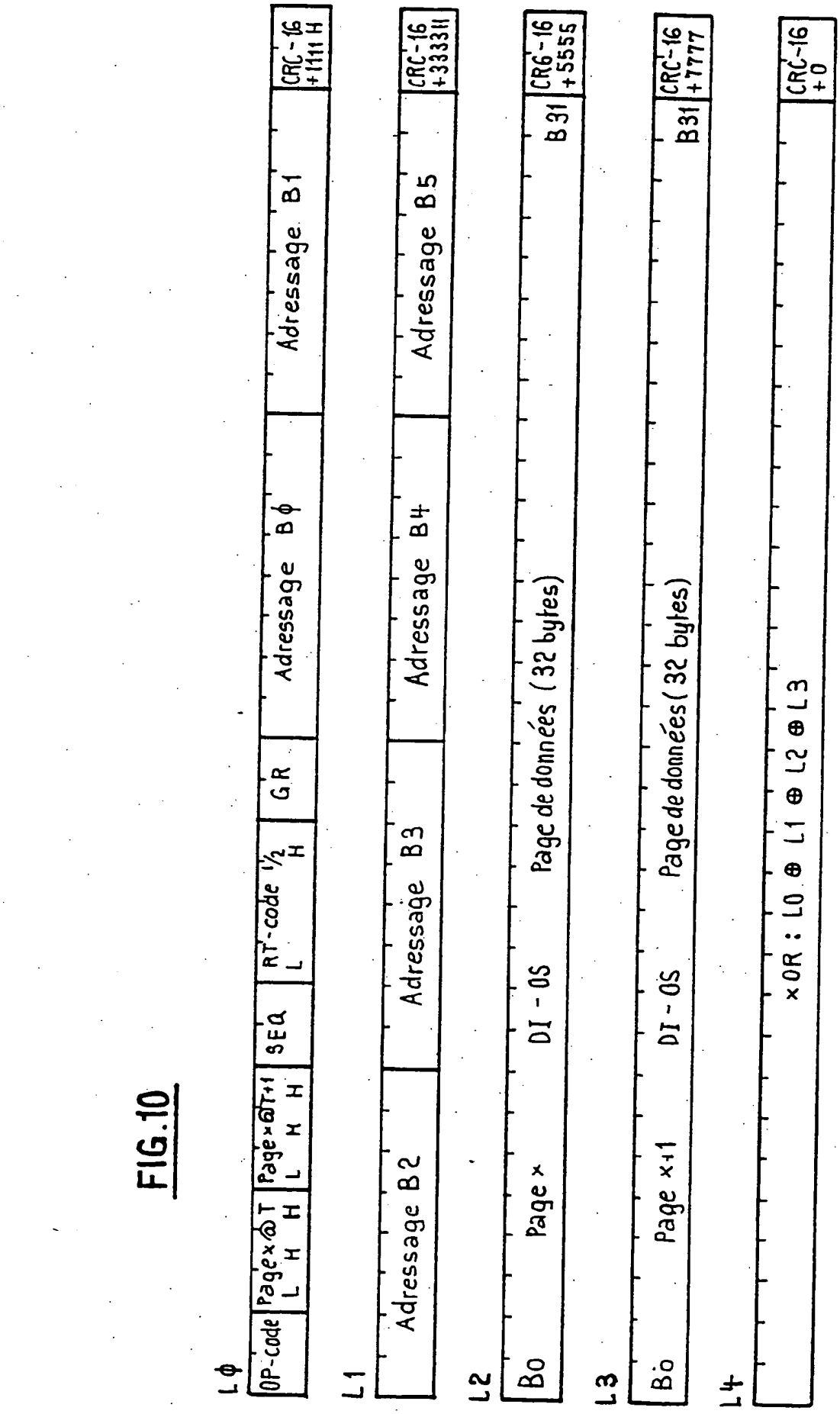
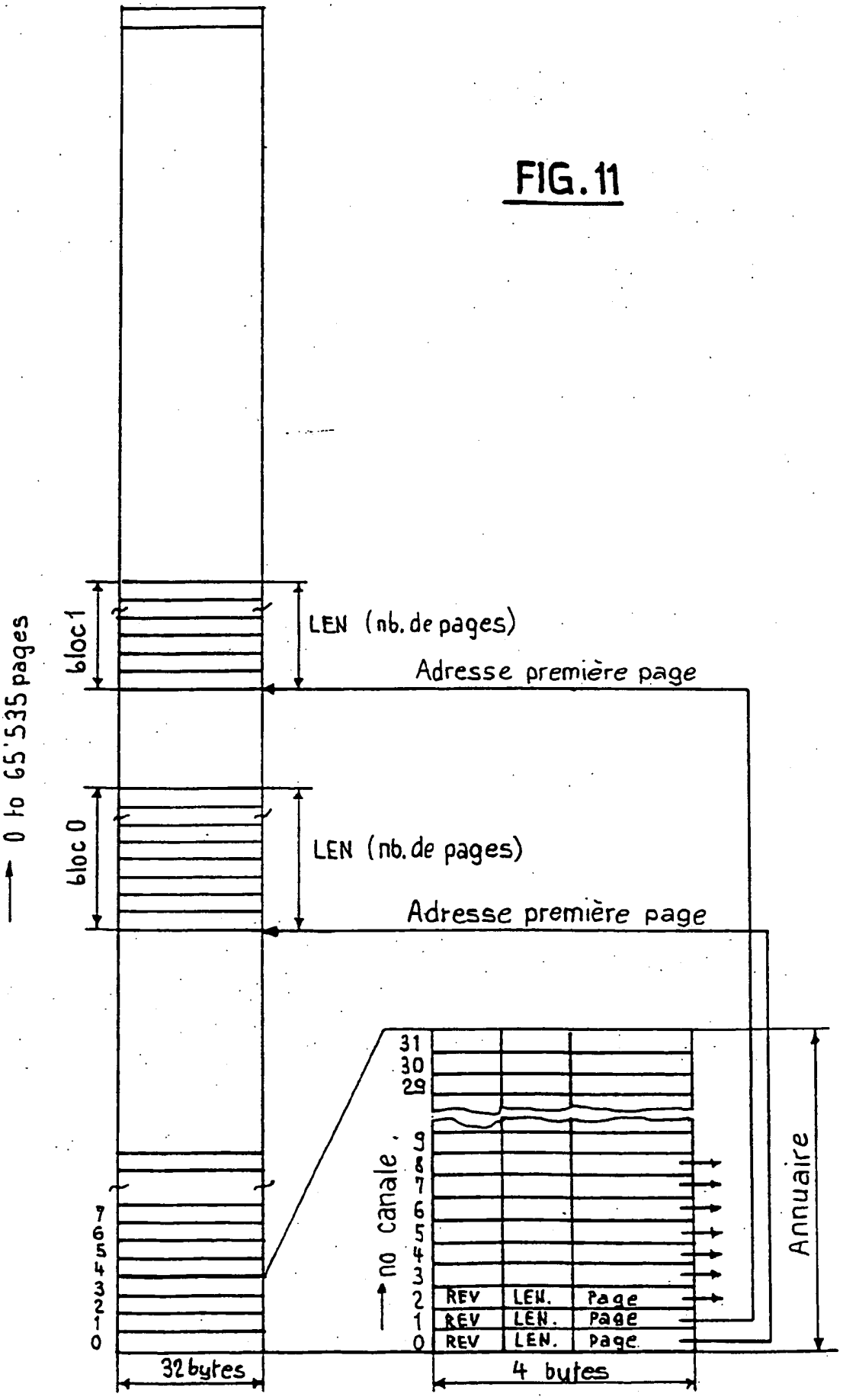

L0
OP-code
Page x @T L H H
Page x @T+1 L H H
SEQ
RT-code 1/2 L H
GR
Adressage Bϕ
Adressage B1
CRC-16 +1111 H
L1
Adressage B2
Adressage B3
Adressage B4
Adressage B5
CRC-16 +33331
L2
B0
Page x
DI - 0S
Page de données (32 bytes)
B31
CRC-16 +5555
L3
Bi
Page x+1
DI - 0S
Page de données (32 bytes)
B31
CRC-16 +7777
L4
×OR : L0 ⊕ L1 ⊕ L2 ⊕ L3
CRC-16 +0

FIG.11


0 to 65'535 pages
bloc 1
LEN (nb. de pages)
Adresse première page
bloc 0
LEN (nb. de pages)
Adresse première page
no canale
31
30
29
9
8
7
6
5
4
3
2
1
0
REV
LEN.
Page
REV
LEN.
Page
REV
LEN.
Page
Annuaire
32 bytes
4 bytes

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 94 11 2343

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
X A	INT. CONF. ON SECURE COMMUNICATION SYSTEMS, 23 Février 1984, LONDON, GB pages 71 - 78 S.M. EDWARDSON 'Scrambling and encryption for direct broadcasting by satellite' * page 72, colonne de gauche, ligne 41 - colonne de droite, ligne 21 * * page 73, colonne de gauche, ligne 65 - colonne de droite, ligne 27 *	1,2 4-9	H04N7/167
Y	EP-A-0 014 654 (ETABLISSEMENT PUBLIC DE DIFFUSION DIT <<TELEDIFFUSION DE FRANCE>> ET A) * le document en entier *	1,2	
Y A	EP-A-0 126 495 (LA RADIOTECHNIQUE) * abrégé *	1,2 4-9	
			DOMAINES TECHNIQUES RECHERCHES (Int.Cl.4)
			H04N

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	3 Octobre 1994	Hazel, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C03)

European Patent

Publication No. : 0 626 793 A1

EUROPEAN PATENT APPLICATION

Application Number: 94112343.2

Int. Cl.[5]: H04N 7/167

Application Date: 14 April 87

This application was filed on 8 August 1994 as required by the application division under code INID 60

Priority: 18 April 86 CH 1576/86

Publication date of application: 30 November 94 Bulletin 94/48

Number of initial publication of application in article 76 CBE : 0 243 312

Designated treaty countries: BE CH DE ES FR GB IT LI NL SE

Applicant: NAGRA PLUS S.A.
22 route de Genève
CH-1033 Cheseaux-sur-Lausanne (CH)

Inventor: Kudelski, André
Chemin de la Crésentine 21
CH-1023 Crissier (CH)

Inventor: Laffely, Laurent
Chemin du Mottier 4
CH-1052 Le Mont-sur-Lausanne (CH)

Inventor: Sasselli, Marco
Chemin des Roches 6
CH-1803 Chardonne (CH)

Fee television system.

A fee television system includes on the reception level a decoder and a separate card (12) which may be connected to the decoder, the decoder receiving at the same time a scrambled video signal and an encoded unscrambling code. The decoder includes a memory (9) intended to store a video signal which arrives scrambled at the decoder, and a first microprocessor (11) intended to control said memory (9) to unscramble the video signal, this first microprocessor (11) being in connection with the separate card (12). This card (12) includes a second microprocessor (40) with a memory (41, 42, 43) designed to store the codes related to the programs purchased, to receive the unscrambling code and to transmit to the decoder the decoded unscrambling code. This decoder uses then the decoded unscrambling code to unscramble, with the aid of the memory (9) the scrambled video signal and to permit therefore a display in clear of the transmitted broadcast.

Fig. 3.

The present invention concerns a fee television system including on the level of the receiver a decoder and a separate card which may be connected to the decoder, the decoder receiving at the same time a scrambled video signal and an encoded unscrambling code.

In a fee television system (pay TV) and very generally, the subscriber chooses the programs he wants to watch and he pays to receive these programs which are broadcast in scrambled form in order to be unintelligible to non-subscribers or to the subscribers who have not chosen nor paid for a particular program. The signals may be transmitted by cable, antenna, or satellite. The fee television systems developed include moreover the possibility, referred to as "pay per view", of buying programs either just before the beginning of the broadcast or during the broadcast, and this in a single path transmission system. In this case it is necessary to store a certain credit at the address of the user, which credit is available to permit the purchase and the reception of a pay per view broadcast which one wants to watch. If the stored credit balance is sufficient, the amount of the broadcast is debited from the credit and the signal received from the broadcasting station is unscrambled to permit convenient reception.

The document WO 81/02499 concerns a procedure and a system for scrambling the broadcast of video information, especially for fee television. Parts of the video signal, for example parts or segments of lines, lines or frames are transmitted in an order different from their natural sequence. The manner of rearranging the sequence of the segments of lines for the broadcast may be controlled by a code generator which changes the sequence at each frame or as a function of another adequate time base. The code, which may be encoded, varies randomly and it may be entirely or partially transmitted with the scrambled video signal.

US patent 4,484,217 concerns a procedure and a system for billing remotely a fee television program. The available credit is stored at the site of the subscriber and a

television program. The available credit is stored at the site of the subscriber and a cost signal is transmitted by the broadcaster. Pay per view is made possible by the fact that there is provided the opportunity for an impulse purchase. For the purpose of identification a single code may accompany the signal emitted. If the decoder of the subscriber recognizes the program as a purchase program on impulse, the cost of the program is displayed. To watch the program the subscriber enters an adequate request in the decoder and the latter automatically compares the cost of the program with the available credit. If the cost does not exceed the credit, the program is unscrambled and the cost is deducted from the credit balance. However, the above system is not equipped to permit displaying in the form of Teletext the information broadcast related to the broadcasts anticipated in their chronological order, nor the display of information in the form of instructions for the operations to be performed by the user on the decoder in order to facilitate the dialogue between the latter and the user and avoid errors of handling.

Consequently, the purpose of the present invention is to improve the managing of credit in a fee television system. For this purpose the decoder of the system includes:

- a memory intended to store a video signal which reaches the decoder in scrambled form and to output said video signal in unscrambled form; and,

- a first microprocessor intended to control said memory to unscramble said video signal, this first microprocessor being in connection with said card.

Moreover, said card includes:

- a second microprocessor with memory intended to store the codes related to the purchased broadcasts to receive said unscrambling code and transmit to the decoder said unscrambling code in decoded form, this decoder then using said decoded unscrambling code to unscramble with the aid of said memory,

said scrambled video signal and thus permit a display in clear of the transmitted broadcast.

The invention will be explained below with reference to the description of one embodiment depicted in the drawing.

Figure 1 shows the fundamental principle of a fee television system.

Figure 2 shows the principle of the input and of the output of a line of the video signal among the 32 lines, for example, from a buffer.

Figure 3 shows a block diagram of the decoder according to the invention.

Figure 4 shows the principle of encoding and decoding of the scrambling codes transmitted.

Figure 5 shows the rotation of a line of the video signal.

Figure 6 shows the inversion of a line of the video signal.

Figure 7 shows the mirror symmetry of a video signal line.

Figure 8 shows a block diagram of the CPTV card.

Figure 9 shows the physical structure of a video signal line.

Figure 10 shows the structure of physical data in the Didon data transmission system; and,

Figure 11 shows the structure of data in the Didon system.

In Figure 1 a microcomputer 1 is provided for generating the data according to a Teletext format related to the programs of the broadcasts provided such as title, price, date or period of broadcast, etc., as well as other information useful to the user. These data are introduced at 3 by an interface 2 into the video signal delivered by a camera 4 or any other element producing a video signal. The lines of the vertical sweep return of the video signal which do not normally transmit any information are used to transmit the Teletext data so that the latter are transmitted at the same time as the video signal.

Figure 9 shows the structure of a vertical sweep return line of the video signal. It can be seen that the line is formed of 32 bytes of Teletext data and that it includes moreover information on synchronization and addresses in Hamming code for the detection / correction of errors. The 32 bytes of Teletext data are protected by 2 bytes of CRC-16 error detection code.

In this example the video signal with the Teletext data is then supplied to a scrambler 5 which permits scrambling the picture, for example by permutation of the lines or by other means. The scrambled signal is transmitted by hertzian path, by video cable, or by satellite to the receiver 6 of the subscriber. The receiver contains a descrambler 7 which delivers the unscrambled signal to the television 8.

The scrambled signal is entirely compatible with the PAL (NTSC) and SECAM standards. The scrambling may be performed in normal version or in deep version. In normal version, the video lines are permuted among themselves, only the active part of the line being permuted. In the PAL (NTSC) system, the burst (color carrier frequency) is left unchanged. Each line is sampled and digitized over 8 bits at a sampling frequency of $f = 3 \times f_{burst}$ or $f = 4 \times f_{burst}$ at the line frequency so that in the PAL (NTSC) system the color phase is retained. Each line is thus divided in principle into 3 (or 4) x 256 segments of 8 bits. Figure 4 shows the principle of scrambling and unscrambling the transmitted video signals. Upon broadcast, a random generator 25

produces code words in real time. Information 26 related to the identification of the broadcast to transmit is delivered with a transmission key 34 and the code word to a system of encoding 27 which delivers in real time [the] encoded signal 28 to be transmitted. The transmission key 34 may be transmitted in coded form. Upon reception the transmitted signal is delivered with the transmission key to the decoding system 29, for example according to the DES system which delivers the decoded code word (as long as the transmission in progress was purchased) and the identification information 26. The code word controls a pseudo-random generator 30 which in turn delivers pointers 31 for a table 32 of 256 permutation codes. At each line of the video signal the table selects among 32 buffers that buffer which permits the depermutation of the lines.

It is possible to enter and output lines from the buffer in any order. Figure 2 shows schematically a buffer memory 18 containing the 3 x 256 segments 19 of 8 bits forming one line of the video signal. In this memory the segments or samples are introduced sequentially into the successive positions of the memory. The figure shows that the introduction of a new segment 20 into one of the memory positions releases the segment 21 which was stored at that position so that the memory is always filled with 32 lines and that a buffer is always filled with 256 segments. The scrambling / unscrambling, such as indicated above, offers an excellent security against piracy for the following reasons:

- The number of line permutations possible is so great that it is difficult to find the "right combination" either randomly or by correlation.

- The permutation key or code is transmitted in real time so that even if a pirate finds the right permutation, the latter is only valid for an instant, for example one second.

- The permutation code is transmitted encoded, for example but not exclusively, according to the DES system, practically unbreakable.

- The decoding of the permutation codes is done on an intelligent microprocessor card (CPTV card) as will be seen below, offering all of the security necessary. According to the invention the microprocessor of the card constitutes one of the elements of the decoder.

- The CPTV cards are reprogrammable, which permits periodically changing the encoding keys.

In the deep scrambling version, there is performed besides the permutation of the lines as indicated above, one or more of the following scrambling processes:

- According to Figure 5, a rotation of the active line on itself, i.e. for example the active part of the line begins in the middle of the true line and is followed after the end of the true line by the beginning of this same line.

- According to Figure 6, an inversion of the polarity of the active line relative to the level corresponding to 50 IRE. This operation permits making an automatic adaptation of the level of luminosity to keep the latter constant. This permits eliminating the possibility of recognizing the picture by changing the environmental lighting.

- According to Figure 7, a mirror symmetry of the video line according to which the active part of the video line undergoes an axial symmetry of the axis perpendicular to the black level of the video.

It will be recalled further that during the scrambling only the active part of the line is permuted, whether or not it includes the vertical sweep return lines, which permits

the scrambling of the Teletext data, but that in all cases the horizontal synchronization remains unchanged. At the output of the buffer the data are reconverted into analog signals by a digital - analog converter of 8 bits. There is thus obtained an unscrambled PAL (NTSC) or SECAM signal for display on the television screen. The principle of the decoder and its possibilities of use will now be examined.

Figure 3 shows that the video signal coming from the head station (broadcaster) is delivered to the video buffer memory 9 of 32 lines permitting making the de-permutation of the lines as indicated above and to a Teletext data receiver 10. It will be recalled here that the data in Teletext format are transmitted at the same time and by the same channel as the video signal, these data being transmitted by the vertical sweep return lines of the video signal. A microprocessor 11 is the central element of the decoder. It includes ROM and RAM for all information which can be displayed on the television screen, this information which is in the form of data in Teletext format being in part transmitted by the head station and stored in a RAM of the microprocessor and in part stored in a ROM of the microprocessor 11. The microprocessor is associated with a security card called CPTV (card for pay TV) 12 normally inserted in the decoder and with a key 13 of the latter. The microprocessor delivers on call with the aid of the keyboard the Teletext data in digital form suitable for a text generator 14 controlling the display of the television. The microprocessor 11 in connection with the CPTV card 12 controls the buffer 9 for depermuting the lines as previously indicated. The unscrambled video signal as well as the text generator are available in 15 to be displayed on the television. Moreover, the microprocessor may also be connected to a modem 16, the latter, in turn, being connected to a telephone line 17.

The possibilities of the decoder described above will now be examined in greater detail.

The CPTV card is an active card including a microprocessor equipped internally with a non-volatile memory (RAM with battery, NVRAM or E2PROM), which cannot be read from the outside (security), and a clock. According to Figure 8 the card includes two electronic circuits A and B; circuit A is a security device with a CPU 40 and associated memories such as ROM 41, E2PROM 42, RAM 43, as well as a memory interface 44, and the circuit B is a separate E2PROM memory of 2 kilobytes. The card is in principle in the form of a credit card. It brings together the following four functions:

- Decoding of the permutation key transmitted in encrypted form, for example according to the DES system.
  The card receives from the microprocessor 11 the encrypted key and returns, if the broadcast has been purchased, the unscrambling key permitting depermuting the video signal lines.

- Storage of the list of numbers or codes of the purchased broadcasts and subscriptions to a particular type of broadcasts (sports, cultural, movie, cooking, etc. broadcasts). This storage of the list of purchased broadcasts permits the CPTV card to return to the microprocessor the unscrambling code only if the broadcast was, in fact, actually purchased. Moreover, and for the purpose of statistics and billing, it is possible to know the purchased broadcasts.

- Credit management. The CPTV card stores information representing the credit which it may use for the purchase of broadcasts or subscriptions. To purchase a broadcast, the user causes to appear by the action on the keyboard 13, the list of broadcasts received in advance from the head station and stored in the microprocessor 11 of the decoder and which are selected by the menu and displayed on the television screen. The television displays, apart from the title of the broadcast, its number, price, broadcasting date, and other useful

information if appropriate. The user then selects the number of the broadcast which he wants by actuating the corresponding key on the keyboard. If the available credit stored in the card is sufficient for the purchase in question, the broadcast or the subscription purchased is stored in the card on the list of purchased broadcasts and the corresponding amount is deducted from the available credit. When the purchased broadcast is transmitted, it is identified by the card by comparison with its number or code entered on the list of purchased broadcasts and the card returns to the microprocessor the code or key for unscrambling.

- The fourth function of the CPTV card is a function of registering the time with a clock. This function is used during certain broadcasts, for example interactive games between the user and the head station, as described later.

It can be seen that the card is distinguished from known cards in prior art in that it stores all of the confidential or secret information necessary for the unscrambling of the video signal, such as unscrambling keys and credit. The cart manages the credit, stores the purchased broadcasts, and permits the unscrambling of the purchased broadcasts. It is erasable, all of the stored data being capable of being modified. It is therefore possible to modify the unscrambling keys and to reuse the card once it is filled.

For all of the operations to be performed, the user is guided by the decoder itself which displays the texts and instructions for handling on the television by means of the text generator 14. For this purpose, a part of the information which can be displayed in the form of text is stored permanently in a ROM of the microprocessor 11, this part corresponding in principle to handling instructions, and the other part of the information is stored temporarily in a RAM of the microprocessor 11, this second packet of information being broadcast by the head station and concerning more particularly the programs which will be broadcast. The following possibilities are

offered to the user:

- Display of titles, prices, etc., of the programs which will be broadcast.
- A guide to the purchase of scheduled broadcasts.
- A guide to the purchase of subscriptions (windows / channels).
- A guide to the functions attached to the decoder.
- A dialogue with the decoder which is transparent to the user.
- Reception of messages (special / general).
- Reception of the standard Teletext.

The foregoing shows that the dialogue between the user and the decoder is considerably facilitated by [the] latter. The decoder is moreover especially well adapted to the purchase by the user, directly at his place, of a broadcast in dialogue with the decoder (pay per view) without informing the management center of it, i.e., all of the purchasing operations are carried out on the CPTV card, the decoder interpreting the commands given by the user and transmitting them to the CPTV card. For this purpose the user simply selects with the aid of the keyboard the title of the broadcast which interests him by entering the number of the latter and actuating a "validation" key. If the credit contained in the CPTV card is sufficient, the number or the code of the broadcast chosen is stored on the list of purchased broadcasts, the corresponding amount is deducted from the available credit, and when the broadcast is aired, the card delivers to the microprocessor the code for unscrambling the broadcast. This principle avoids an overuse of the telephone lines and permits a user to buy a broadcast in progress.

If the credit contained in the card is zero or insufficient for the purchase of a subscription or of a broadcast, a new credit or an increase of credit still available may be introduced into the card according to the following possibilities:

- Purchase by the user at the management center of a code (for example of 9

digits) corresponding to the amount of the credit to be recharged and reloading of the credit by the introduction of this code into the decoder with the aid of the keyboard. When the code is introduced into the decoder the new credit is stored in the CPTV card.

- By mail exchange of the card at regular times, which permits the head station to know what programs have been watched (statistics).

- Reloading of the credit at a point of sale (video club, bank), likewise permitting knowing what programs were watched.

- By remote control: the credit of the card may be reloaded by antenna or by cable on ordering the broadcast.

Among the possible uses of the decoder according to the invention are further mentioned:

- Display of menus for the purchase of subscription programs with the possibility of knowing at all times the programs purchased, these programs being designated by a particular symbol (letter, digit), display of the further credit available, the expiration dates of the subscriptions, the overall offer by the head station, i.e. updating of programs which will be broadcast subsequently, change of conditions by group of subscribers, etc. All this information which is delivered by the Teletext data receiver (10) is stored in the memories of the microprocessor 11 and displayed on demand on the television screen by the text generator 14.

- Interactive games: This involves for example a game of lotto with the head station in which the user participates by showing a number and introducing the corresponding amount played with the aid of the keyboard 13. The number and the amount played are stored in the CPTV card. The number

drawn or coming out of the broadcast is transmitted by the video signal and in coded form as Teletext data and it corresponds to the number entered by the user, the latter is authenticated by the CPTV card with the aid of the internal clock which it contains and which determines exactly the time elapsed between the entering and the check of the win to prevent any fraud, it being well understood that the entering must precede the drawing and broadcast. If the player is a winner, the decoder calls the broadcasting center by way of the modem 16 and the win is awarded in the form of an increase in credit in the CPTV card, this increase being ordered by the head station (see below).

- Reception of personalized messages issued by the head station. These messages are sent in a Teletext format and the decoder verifies that it really is authorized to receive the message. For this purpose each CPTV card is the carrier of a particular stored identification number which is transmitted [to or from the] head station with each message. If the decoder is indeed the one to which the message is addressed, the card permits the display of the message on the television set.

- Security code. This involves a code intended to prevent unauthorized persons, for example children, from making purchases whose amount exceeds a predetermined amount or participating in games which are not intended for them. In this case it is necessary to introduce by the keyboard a security code into the decoder, such as a password. If the latter is not entered or if it is not correct, the decoder refuses to execute the order which it is given.

- Connection by modem. Due to the modem 16 connected to the microprocessor 11 and to a telephone line 17, it is possible for the decoder, into which the CPTV card is inserted, to call automatically during the night (due to the clock of the CPTV card) the head station to have a credit reloaded if the latter is depleted. On the same occasion the decoder sends to the head station the set

of broadcasts watched. Of course, the calling of the head station by the decoder may also be done periodically on set dates if desired.

- The decoder may be used as a standard Teletext receiver with all of the usual functions of the operators of television networks or with the postal, telecommunications, and broadcasting service.

Figure 10 shows as an example of the organization of data in the video signal lines the structure of the physical data in the case of a transmission of data by the Didon system (France). At each frame of the video signal there is transmitted a line such as L0, L1, L2, L3, or L4. Thus, a group of 5 lines (L0 through L4) is transmitted every 5 frames. It is seen more particularly that the lines L2 and L3 transmit pages of data of 32 bytes each. The addresses B0 through BS permit selecting a group of subscribers from among 2exp24 groups, each of 240 subscribers. The addresses include a group number, the action to perform, for example reloading credit, and the list of subscribers concerned by this particular action. Synchronization is ensured by a remainder of CRC-16 as indicated. Moreover, each line is protected by a CRC-16 which permits an error detection and each group of 5 lines is protected by an exclusive OR which permits correcting an erroneous line. The advantage of a data organization according to Figure 10 it that it permits recovering very quickly the information there where it is located in the decoder.

Figure 11 shows another example of data structure in the case of the DI-OS system (Didon operating system). It is seen that the data are organized in 65,536 pages of 32 bytes each. The first four pages (0 through 3) of the data structure include a table which delivers for each channel which can be transmitted the address of the first page of a block of pages corresponding to this channel as well as the length of the block which is identical to the number of pages of this block and the number of revisions or modifications which have been given to this block. The advantage of the organization according to Figure 11 is that it leads to a very flexible structure for the

transmission of data as well as a very flexible future expansion.

The foregoing shows that the decoder according to the invention offers a very large number of possibilities to the user, and, more particularly, that it facilitates the dialogue with the latter due to the display on the television of the programs of broadcasts provided and of handling instructions necessary to carry out on the keyboard for their purchase or a reloading of credit. Moreover, the CPTV card makes the decoder extremely secure against piracy.

Patent Claims

1. A fee television system including on the level of reception a decoder and a separate card (12) which can be connected to said decoder, the decoder receiving at the same time a scrambled video signal and an encoded unscrambling code, characterized in that:

said decoder includes:

- a memory (9) intended to store a video signal which reaches the decoder in scrambled form and to output said video signal unscrambled; and,

- a first microprocessor (11) intended to control said memory (9) to unscramble said video signal, this first microprocessor (11) being in connection with said card (12);

and in that said card (12) includes:

- a second microprocessor (40) with memory (41, 42, 43) intended to store the codes related to broadcasts purchased, to receive said unscrambling code, and to transmit to the decoder said encoded unscrambling code; this decoder then using said decoded unscrambling code to unscramble with the aid of said memory (9) said scrambled video signal and to permit thereby a display in clear of the transmitted broadcast.

2. A fee television system according to claim 1, characterized in that upon broadcast, code words, information (26) related to the identification of the broadcast to be transmitted, and a transmission key (34) are generated and sent to an encoding system (27) which supplies in real time the encoded signal (28) to be transmitted and upon receipt the transmitted signal is delivered with the transmission key to a decoding system (29) which delivers the decoded code word and the identification information (26), the code word controlling a pseudo-random generator (30) which, in turn, supplies unscrambling codes for unscrambling in the decoder the received scrambled video signal.

3. A fee television system according to claim 2, characterized in that said decoded unscrambling code controls the pseudo-random generator (30) which delivers, in turn, pointers (31) to perform the pointing on a table (32) constituted by a number of unscrambling codes such that the unscrambling codes pointed to are used to control said memory (9) for it to output said video signal in unscrambled form.

4. A fee television system according to claim 1, 2, or 3, where the memory (9) of the decoder is enabled to receive a video signal scrambled by the permutation of lines in which each line is sampled and digitized in a number of samples, and means for unscrambling the stored video signal according to a variable unscrambling code, characterized in that said memory (9) is constituted of a buffer of lines (18), for example 32 lines, where said samples (20) are introduced sequentially into the successive cells (19), each line (18) of the buffer being constituted of as many cells as are necessary for storing the number of samples (20, 21) of one line of the video signal, the input of each sample (20) into a cell of the buffer causing the output of this cell of the sample (21) stored in this same cell, so that said memory (9) is always filled with the number of lines and that each line of the buffer (18) is always filled with the number of samples (21 or 20) which it can contain, the order of

extraction of the lines from the buffer stored (18) to do the unscrambling being determined by the selection under the control of said unscrambling code from among the lines of the buffer, of those which permit the depermutation of the lines.

5. A fee television system according to claim 4, characterized in that each line of the digitized video signal includes 3 or 4 times 256 samples of 8 bits each, these samples coming to be stored in an equal number of cells (19) of a line (18) of the buffer.

6. A fee television system according to either of the claims 4 or 5, characterized in that the buffer contains 32 lines.

7. A fee television system according to any of the claims 4 through 6, for the decoding of a video signal in which data are stored on the vertical sweep return lines and only the active part of the line is permuted, including the vertical sweep return, the horizontal synchronization not being permuted so that said data are scrambled at the same time as the picture.

8. A fee television system according to any of the claims 4 through 7, for the decoding of a video signal in which, in addition to the permutation of the lines, each line thus permuted undergoes moreover a rotation of the active part of the line upon itself.

9. A fee television system according to any of the claims 4 through 8, characterized in that the means for unscrambling the video signal include: a system for decoding (29) a CPTV card delivering a decoded code word, and a pseudo-random generator (30) which delivers pointers (31) to a table (32) containing a number of permutation codes, which table selects from among the lines (18) of the buffer those which permit depermutation.

Fig. 9.

Characteristics

Transmission speed: 6,203,135 Mbits/sec.

Code: NRZ, AM

Put into form: sine squared.

Line of data: 320 bits - 40 bytes.

Sequential order of data: LsB ... MsB; LsB ... MsB.

PLL synchronization: 2 x 55 H.

Synchronization byte: E7 H

Address; A1, A2, A3 bytes in Hamming code.

Protection: The 32 bytes are protected by 2 bytes of CRC-16.

hex value

Hamming byte

Fig. 10.

B0 addressing
B1 addressing
B2 addressing
B3 addressing
B4 addressing
B5 addressing

Page of data
Page of data

Fig. 11

(Number of pages)

First page address

(Number of pages)

First page address.

European Patent Office

Number of Application:

European Search Report

EP 94 11 2343

Relevant Documents

Category	Identification of Documents with specification, where required of critical parts	Re Claim	Classification of Appl. (Int.Cl.[4])
X	INT. CONF. ON SECURE COMMUNICATION SYSTEMS, 23 February 1984, LONDON, GB Pages 71 - 78 S.M. EDWARDSON 'Scrambling and encryption for direct Broadcasting by satellite'	1, 2	H04N7/167
A	* page 72, left column, lines 41 to right column, line 21 * * page 73, left column, line 65 to right column, line 27 *	4-9	
Y	EP-A-0 014 654 (ETABLISSEMENT PUBLIC DE DIFFUSION DIT <<TELEDIFFUSION DE FRANCE>> Et a) * entire document *	1, 2	
Y	EP-A-0 126 495 (LA RADIOTECHNIQUE)	1, 2	
A	* Abstract *	4-9	

Searched Fields (Int. Cl [4])
H04N

The present search report was completed for all patent claims

Place of Search	Search completed	Examiner
DEN HAAG	3 October 1994	Hazel , J.

Category of cited documents

X of special significance considered alone
A technology background
Y of special significance in combination with another document of the same category